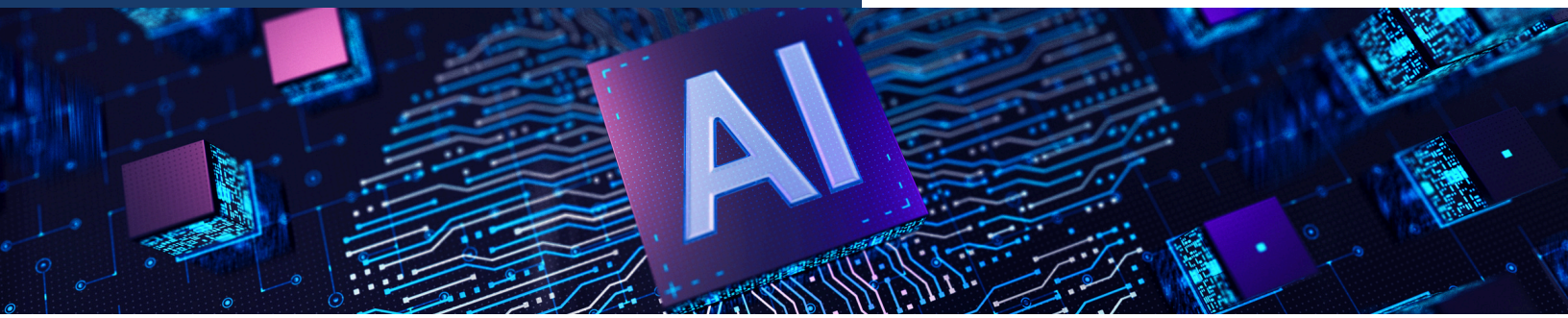
LAW ALERT
June 22, 2026
By: Adam H. Russ, Esq.
Kyle N. Voigt, Law Clerk

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.



AI Is Not Your Lawyer: Public Prompts May Waive Privilege

United States v. Heppner, 2026 WL 436479 (SDNY February 17, 2026), highlights the privilege and work-product risks that arise when clients use public generative AI tools in litigation or investigations.

Do Not Treat Public AI as Private

In-house legal teams, executives, and employees should not assume that AI prompts about litigation, investigations, regulatory issues, or legal strategy are private. In *United States v. Heppner*, Judge Jed S. Rakoff of the Southern District of New York held that a defendant's exchanges with a public AI tool were not protected by attorney-client privilege or work product. The practical lesson is clear: without counsel supervision and confidentiality protections, dispute-related AI prompts and outputs may become discoverable.

How Public AI Use Created a Privilege Problem

After receiving a grand jury subpoena and learning he was a target of a federal investigation, Bradley Heppner used Claude, a public AI tool operated by Anthropic, to prepare materials addressing possible defense strategy, factual arguments, and legal issues. The materials were later shared with counsel. Heppner asserted privilege, arguing that he had entered information learned from counsel, created the materials to facilitate legal advice, and ultimately provided them to his lawyers. The court rejected those arguments and permitted government review of Heppner's AI documents.

What This Means for Your Business

- Public AI tools may be treated as outside third parties. If your employees enter legal strategy, privileged advice, or dispute-sensitive facts into a public AI tool, a court may treat the information disclosed as outside the attorney-client privileged relationship.
- Privilege may be waived before counsel ever sees the document. Even if the information originated in privileged conversations, entering it into a public AI tool may waive protection.
- Later forwarding AI output to counsel may not cure the waiver. Sending AI-generated materials to a lawyer after the fact does not automatically make them privileged or shield them from discovery.
- Work product protection is strongest when counsel directs the process. AI use is less defensible when employees use public AI tools on their own initiative rather than as part of a counsel-supervised legal workflow.
- Secure, counsel-directed AI use may be treated differently. The safer path is to use approved tools, document attorney supervision, and maintain clear confidentiality controls.

Ground Rules for Using AI Safely

- Do not treat public AI tools as confidential legal workspaces. Attorney advice, legal strategy, deposition preparation, investigation facts, settlement positions, and regulatory response materials should not be entered into public AI tools.
- Use AI for legal work only within a counsel-approved workflow. AI use is safest when counsel approves the tool, defines the permitted use, supervises the process, and confirms that appropriate confidentiality protections are in place.
- Treat AI prompts and outputs as potential records. In active disputes, investigations, and regulatory matters, prompts, outputs, drafts, and related communications may need to be preserved and may be subject to discovery.

The Inadvertent Waiver Risk

The immediate danger for clients is inadvertent waiver. Employees may think they are simply organizing thoughts, summarizing facts, or preparing for a call with counsel. But if they do that in a public AI tool, a court may treat the prompt (and any output) as a disclosure to a thirdparty. Until courts provide more guidance, companies should assume that unsupervised AI use in disputes, investigations, or regulatory matters can create discoverable records and undermine privilege.

Privilege Protection Checklist

1. Issue clear instructions to relevant employees that public AI tools may not be used for litigation, investigations, regulatory issues, or privileged matters unless counsel approves the use in advance.
2. Update litigation-hold and investigation notices to address AI prompts, outputs, drafts, and related records, including preservation obligations and deletion restrictions.
3. Inventory AI tools used by legal, compliance, finance, HR, and executive teams, and confirm retention, review, sharing, training, access-control, and vendor-use terms.
4. Create approved-use guidelines that specify which tools may be used, who may use them, what categories of information are prohibited, and when counsel supervision is required.
5. Train legal-adjacent business teams with practical examples of prohibited prompts, including attorney advice, legal strategy, confidential facts, settlement positions, and dispute-sensitive summaries.

Before You Prompt, Protect Privilege

Heppner does not mean AI is off limits for legal work. It does mean that clients and employees should treat AI use in litigation, investigations, and regulatory matters as a privilege and confidentiality issue from the outset. Public, unsupervised prompting can create discoverable records at the exact moment confidentiality matters most. Before using AI tools for any legal or dispute-related purpose, involve counsel, use approved tools, and document the safeguards.

Adam H. Russ, Esq.
516-663-6557
aruss@rmfpc.com